Deutscher Bundestag **Drucksache 17/5659**

17. Wahlperiode 27. 04. 2011

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jan Korte, Karin Binder, Caren Lay, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/5407 –

Schutz vor PIN-Skimming

Vorbemerkung der Fragesteller

Am 2. Januar 2011 berichtete die „Frankfurter Allgemeine Sonntagszeitung" (FAS), dass das Bundeskriminalamt (BKA), als Maßnahme gegen das 2010 stark angestiegene Ausspähen der Daten von EC- und Kreditkarten an Geldautomaten (Skimming), eine flächendeckende Einführung magnetstreifenloser Debitkarten fordert.

Seit dem 1. Januar 2011 werden die Transaktionen zwischen Karte und Geldautomat im Euro-Raum von einem EMV-Chip abgewickelt, der die im Magnetstreifen enthaltenen Daten verschlüsselt speichert und das Fälschen von Karten unmöglich machen soll. Trotzdem haben die meisten EC- und Kreditkarten auch weiterhin zusätzlich einen Magnetstreifen, damit die Geldkarten auch außerhalb des einheitlichen Euro-Zahlungsraumes eingesetzt werden können.

In ihrer am 9. März 2011 vorgestellten Präsentation „Credit Card skimming and PIN harvesting in an EMV world" (http://dev.inversepath.com/download/emv/emv_2011.pdf) beschreiben vier Forscher, wie sich die Kommunikation zwischen Terminal und Chip durch eine flache Platine im Kartenschlitz belauschen und manipulieren lässt, um an eine PIN zu gelangen.

Dabei sei es laut einem Bericht bei „heise online" vom 16. März 2011 „unerheblich, ob die Karte einen billigen Chip ohne eigene Kryptografiefunktion (SDA) oder einen teuren, bislang als sicher geltenden Chip mit Dynamic Data Authentication (DDA) enthält". Der Bericht zitiert Daniele Bianco, einen der vier Forscher, mit folgender Aussage: „Das eigentliche Problem bei EMV ist, dass durch die scheinbare Sicherheit des Verfahrens die Beweislast auf den Kunden abgewälzt wird. Es wird ihm unterstellt, dass er fahrlässig mit seiner PIN umgegangen ist." Betroffen seien nach Daniele Biancos Ansicht alle EMV-Installationen, demnach auch die in der Bundesrepublik Deutschland.

Von diesen grundsätzlichen Sicherheitsproblemen wissen Hersteller und Banken jedoch offenbar schon seit über fünf Jahren. Am 8. März 2006 berichtete das ARD-Fernsehmagazin „Plusminus" bereits über Schwachstellen von Kreditkarten, die mit der neuen Chiptechnologie ausgestattet sind. Damals

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 20. April 2011 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

demonstrierten Wissenschaftler der Universität Cambridge bereits in einem Skimming-Angriff auf SDA-Karten unter Laborbedingungen, wie sich die Kommunikation der Karte mit einem präparierten Chipkartenterminal abhören lässt. Vor rund einem Jahr zeigten dieselben britischen Forscher zudem einen Weg auf, mit dem sich das EMV-Verfahren bei EC- und Kreditkarten so aushebeln lässt, dass Karten scheinbar beliebige PIN akzeptieren. Diese Manipulation ließ sich allerdings im Nachhinein aufdecken, so dass, anders als bei den neuesten Skimming-Attacken, die Kunden nicht automatisch in Haftung wären (vgl. hierzu auch heise online vom 8. März 2011).

Laut FAS schlägt das BKA im Kampf gegen Skimming den Banken vor, standardmäßig EC- und Kreditkarten ohne Magnetstreifen auszugeben. Lediglich an Kunden, die ihre Karten auch im außereuropäischen Ausland einsetzen wollen, soll auf Antrag eine zweite Karte mit Magnetstreifen ausgehändigt werden, was jedoch nur 5 Prozent der Bankkunden betreffe (FAS vom 2. Januar 2011).

Schon im Juli 2010 hatte das BKA davor gewarnt, dass bei Skimming-Angriffen ein neuer Höchststand bevorstünde. Nach Angaben des BKA wurden bereits im ersten Halbjahr 2010 so viele Skimming-Fälle registriert wie im gesamten Vorjahr und dieser Trend hätte sich auch im zweiten Halbjahr fortgesetzt (vgl. FAS vom 2. Januar 2011).

1. Wie viele Debitkarten sind derzeit bei den in der Bundesrepublik Deutschland lebenden Bürgerinnen und Bürger im Umlauf (bitte nach Kartenart und Ausstattungsmerkmalen aufschlüsseln)?

Der Bundesregierung liegen hierzu keine Informationen vor. Nach Schätzungen der Firma Euro-Kartensysteme GmbH[1] (EKS) sind in Deutschland mehr als 90 Millionen Debitkarten ausgegeben.

2. Wie bewertet die Bundesregierung das derzeitige Risiko von PIN-Skimming in der Bundesrepublik Deutschland, vor dem Hintergrund der aktuell aufgedeckten Sicherheitsprobleme bei der bislang als sicher geltenden DDA-Chipklasse?

Nach Ansicht der Bundesregierung bleibt das Risiko in unverändertem Umfang bestehen. Durch die in der angesprochenen Veröffentlichung beschriebene Methode können unter günstigsten Bedingungen aus dem Chip neben der PIN die gleichen Kartendaten ausgelesen werden, die bisher auch auf die Magnetstreifen codiert sind. Die auf diesem Wege erlangten Daten können – wie bisher – auf den Magnetstreifen einer Kartendublette codiert werden, die dann außerhalb der SEPA[2]-Zone eingesetzt werden kann. Das Missbrauchsproblem besteht also darin, dass Kreditinstitute immer noch Magnetstreifentransaktionen akzeptieren, die außerhalb der sog. SEPA-Länder getätigt werden.

Der Bundesregierung liegen dagegen keine Hinweise darauf vor, dass durch Manipulation erfolgreich ein neuer Chip mit EMV-Standard geklont werden kann, um damit innerhalb oder außerhalb der SEPA-Zone Chip-basierte Transaktionen vorzunehmen.

---

[1] Die EURO Kartensysteme GmbH ist ein Gemeinschaftsunternehmen der deutschen Kreditwirtschaft, das Aufgaben im Interesse aller Banken und Sparkassen erfüllt.

[2] SEPA: Single Euro Payments Area, umfasst alle EU-Mitgliedstaaten, die drei übrigen Länder des Europäischen Wirtschaftsraums (Island, Liechtenstein und Norwegen) sowie die Schweiz und Monaco.

3. Wie viele der sogenannten Skimming-Angriffe, von denen in der Bundesrepublik Deutschland lebende Bürgerinnen und Bürger betroffen waren, wurden seit 2005 vom BKA im In- und Ausland registriert (bitte nach Halbjahr/Jahr, Land, Bundesland und Angriffsart aufschlüsseln)?

	Inland:	Ausland:
2005	219	keine Zahlen erhoben
2006	308	445
2007[3]	1 349	332
2008	2 397	514
2009	2 058	619
2010	3 183	533

Angriffe auf Geldautomaten – Daten werden erst ab dem Jahr 2007 aufgeschlüsselt nach Bundesländern erhoben:

Bundesland	2007	2008	2009	2010
Baden-Württemberg	176	252	124	244
Bayern	60	290	166	195
Berlin	125	204	363	441
Brandenburg	4	28	29	76
Bremen	18	47	19	32
Hamburg	83	112	109	125
Hessen	68	149	151	183
Mecklenburg-Vorpommern	3	20	2	38
Niedersachsen	92	256	160	208
Nordrhein-Westphalen	627	746	661	1 144
Rheinland-Pfalz	75	75	98	118
Saarland	6	8	13	25
Sachsen	0	56	93	115
Sachsen-Anhalt	2	50	8	85
Schleswig-Holstein	10	60	50	86
Thüringen	0	34	12	68

Eine spezifische Aufschlüsselung nach Angriffsart sowie der Auslandsfälle nach Ländern ist mangels Erfassung nicht möglich.

[3] Ab dem Jahr 2007 geänderte Zählweise.

4. Wie hoch beläuft sich der durch die sogenannten Skimming-Angriffe entstandene Schaden seit 2005 (bitte nach Halbjahr/Jahr, Land und Bundesland aufschlüsseln)?

Der Bundesregierung ist bekannt, dass das deutsche Kreditgewerbe einen alle Institutsgruppen übergreifenden Schadenspool betreibt. Dieser Pool wird durch die Firma EKS verwaltet, die mit der Erfassung und Abwicklung von durch ge- oder verfälschte deutsche Debitkarten entstandenen Schäden betraut ist und die von Skimmingtaten betroffenen Kunden aus diesem Pool entschädigt.

Die EKS hatte dem Bundeskriminalamt in den Jahren 2005 bis 2007 – ohne diese nach Bundesländern aufzuschlüsseln – folgende Schadenssummen mitgeteilt:

2005 ca. 7 Mio. Euro

2006 ca. 11 Mio. Euro

2007 ca. 21 Mio. Euro.

Im Jahr 2008 hatte der Zentrale Kreditausschuss beschlossen, für die Zukunft keine Zahlen zur Schadensentwicklung mehr zur Verfügung zu stellen. Das BKA schätzte den in den Jahren 2008 und 2009 entstandenen Schaden auf jeweils ca. 40 Mio. Euro.

5. Wie viele Fälle konnten vom BKA und anderen mit dem Problem befassten Polizeistellen seit 2005 aufgedeckt und aufgeklärt werden (bitte nach Jahr und Bundesland aufschlüsseln)?

Skimmingdelikte werden in der polizeilichen Kriminalstatistik nicht unter einer speziellen Schlüsselzahl erfasst. Daher können keine Aussagen zur Aufklärung dieser Taten getroffen werden.

6. Wer kommt bei Skimming-Attacken aufgrund welcher Rechtslage für den entstandenen Schaden auf?

   In wie vielen Fällen mussten die betroffenen Kunden den Schaden selbst tragen, in wie vielen Fällen gelang es eine Manipulation nachzuweisen, und in wie vielen Fällen wurde der Schaden von den Banken übernommen?

Auf die Antwort zu Frage 4 wird hingewiesen. Der Bundesregierung sind keine Fälle bekannt, in denen Kunden, deren Kartendaten durch Skimming erlangt wurden, den Schaden selbst tragen mussten.

Da der Bankkunde bei erfolgreichen Skimmingtaten keinen Zahlungsvorgang autorisiert hat, besteht gegen ihn in aller Regel kein Anspruch auf Erstattung des Schadens. Dies wird durch § 675u Satz 1 des Bürgerlichen Gesetzbuchs (BGB) klargestellt. Vielmehr muss der Zahlungsdienstleister dem Kunden den Zahlungsbetrag unverzüglich erstatten und sein Konto ggf. wieder auf den Stand ohne die Belastung durch den nicht autorisierten Zahlungsvorgang bringen (vgl. § 675u Satz 2 BGB).

§ 675v BGB regelt abweichend von diesem Grundsatz die Voraussetzungen, unter denen der Inhaber eines Zahlungsauthentifizierungsinstruments den aus dem Missbrauch desselben resultierenden Schaden selbst tragen oder sich daran beteiligen muss. Nach der Vorschrift ist zwischen der missbräuchlichen Nutzung des Zahlungsauthentifizierungsinstruments vor und nach Erstattung einer Missbrauchs- bzw. Verlustanzeige zu unterscheiden.

Ein Verlust des Zahlungsauthentifizierungsinstruments steht bei Skimming-Sachverhalten jedoch nicht im Raum. Vielmehr zeichnen sich diese Sachverhalte dadurch aus, dass der Bankkunde weiterhin in Besitz der Karte ist und lediglich nicht bemerkt hat, dass die Daten durch Manipulation in fremde Hände gelangt sind. In Betracht kommt daher allenfalls eine Haftung des Bankkunden wegen grob fahrlässiger Verletzung seiner Sorgfaltspflichten, die missbräuchliche Verwendung des Zahlungsauthentifizierungsinstruments anzuzeigen. In diesem Ausnahmefalls bestünde ein Anspruch gegen den Bankkunden gemäß § 675v Absatz 2 Nummer 1 BGB i. V. m. § 675l Satz 2 BGB.

Unter einem Zahlungsauthentifizierungsinstrument versteht man gemäß § 1 Absatz 5 des Zahlungsdiensteaufsichtsgesetzes (ZAG) jedes personalisierte Instrument oder Verfahren, das zwischen dem Zahlungsdienstnutzer und dem Zahlungsdienstleister für die Erteilung von Zahlungsaufträgen vereinbart wird und das vom Zahlungsdienstnutzer eingesetzt wird, um einen Zahlungsauftrag zu erteilen. Als solche Instrumente kommen auch Zahlungskarten wie die Girocard (früher: ec-Karte) unter Verwendung der PIN oder die Kreditkarte mit PIN oder Unterschrift in Frage.

Eine Girocard kann ohne Verwendung der PIN zwar im elektronischen Lastschriftverfahren eingesetzt werden. Da bei dem elektronischen Lastschriftverfahren allerdings nur die im Magnetstreifen der Karte befindlichen Kontodaten herausgelesen werden und daraus eine (vom Kunden zu unterschreibende) Einzugsermächtigungslastschrift generiert wird, erteilt der Zahler in diesem Verfahren gerade keinen Zahlungsauftrag und setzt damit kein Zahlungsauthentifizierungsinstrument nach § 1 Absatz 5 ZAG ein (vgl. Bundestagsdrucksache 16/11613, S. 36; Bundestagsdrucksache 16/11643, S. 102). Zu einer Mithaftung des Bankkunden in Höhe von maximal 150 Euro gemäß § 675v BGB kommt es deshalb bei einer missbräuchlichen Verwendung der Karte im elektronischen Lastschriftverfahren nicht.

7. Wie bewertet die Bundesregierung, vor dem Hintergrund der aktuell aufgedeckten Sicherheitsprobleme bei den bislang als sicher geltenden DDA-Chips, die Forderungen des BKA an die Banken, standardmäßig nur noch EC- und Kreditkarten ohne Magnetstreifen auszugeben?

Auf die Antwort zu Frage 2 wird verwiesen. Problematisch sind Auslandstransaktionen, die Banken ausschließlich auf Grundlage der Magnetstreifendaten autorisieren.

8. Wie war nach Kenntnis der Bundesregierung die Resonanz bei den Banken auf die Forderungen des BKA, und was hat sich an der Kartenausgabepraxis seitdem geändert?

Nach Kenntnis der Bundesregierung wurde die Forderung des BKA zur Abschaffung der Magnetstreifen von den Bankenverbänden zur Kenntnis genommen und kontrovers diskutiert.

Anlässlich eines Gespräches im Bundesministerium des Innern hatte der Zentrale Kreditausschuss (ZKA) darauf hingewiesen, dass die Umstellung der Debitkarten auf Chip und die Abschaffung des Magnetstreifens Maßnahmen sind, die vielfältige Auswirkungen haben, insbesondere auch die Servicefunktionen der Karten ohne Magnetstreifen einschränken würden. Die Entscheidung zur Abschaffung der Magnetstreifen auf den Karten trifft jedes Kreditinstitut eigenständig. ZKA und Verbände haben keine zentrale Entscheidungsbefugnis.

Der Bundesregierung ist bekannt, dass einzelne Kreditinstitute zwischenzeitlich ihre Kartenausgabepraxis geändert oder andere Maßnahmen ergriffen haben, z. B.:

– die Umstellung der Debitkarten auf ein ausschließlich Chip-basiertes Verfahren, wonach Karten im Ausland nur über Chiptechnologie einsetzbar sind,

– durch Deaktivierung von Magnetstreifen. Bei Einsatz der Karte in „Nicht-Chip-Ländern“ werden Transaktionen nur dann autorisiert, wenn der Kunde vorher den Magnetstreifen aktivieren lässt,

– durch Reduzierung der seitens der Bank vorgegebenen bzw. durch vom Kunden frei festzulegende Limits für Auslandsabhebungen.

9. Erwägt die Bundesregierung gesetzgeberische Initiativen zur Verbesserung der Sicherheit von EC- und Kreditkarten?

Die Bundesregierung beabsichtigt derzeit keine gesetzgeberischen Maßnahmen.

10. Wie beurteilt die Bundesregierung das geschilderte Beweislastproblem bei EMV, und hat sie bereits Maßnahmen erwogen oder unternommen, um hier die Kunden zu schützen und gegenzusteuern?

Wenn ja, welche waren/sind dies?

Wenn nein, warum nicht?

Wie bereits unter Frage 6 dargestellt, haftet der Karteninhaber nach § 675v Absatz 2 BGB für den gesamten entstandenen Schaden allenfalls dann, wenn er ihn unter mindestens grob fahrlässiger Verletzung der ihm kraft Gesetzes oder vertraglicher Vereinbarung obliegenden Sorgfaltspflichten herbeigeführt hat. Eine leicht fahrlässige Verletzung dieser Pflichten reicht daher nicht aus.

Abgesehen davon, dass die Schäden in der Praxis regelmäßig aus dem in Frage 4 beschriebenen Pool ersetzt werden, müsste das Schadensersatzansprüche geltend machende Kreditinstitut in Fällen des Kartenmissbrauchs nach den gesetzlichen Beweislastregeln die grobe Fahrlässigkeit des Karteninhabers zu beweisen. Aufgrund allgemeiner Grundsätze des deutschen Beweisrechts kann allerdings bei typischen Geschehensabläufen im Wege des Anscheinsbeweises von unstreitigen oder bewiesenen Tatsachen, gestützt auf Erfahrungssätze, auf zu beweisende Tatsachen geschlossen werden. So wird in Fällen, in denen unter Verwendung einer entwendeten Zahlungskarte und Eingabe der richtigen persönlichen Geheimzahl an Geldausgabeautomaten Bargeld abgehoben wird, davon ausgegangen, dass der Karteninhaber die PIN auf der Karte notiert oder gemeinsam mit dieser verwahrt hat. Dies gilt aber nur, wenn andere Ursachen für den Missbrauch nach der Lebenserfahrung außer Betracht bleiben. Der Karteninhaber kann dann Tatsachen darlegen und ggf. beweisen, die die ernsthafte, ebenfalls in Betracht kommende Möglichkeit einer anderen Ursache nahelegen.

Vorbehaltlich der von der Rechtsprechung in jedem Einzelfall vorzunehmenden Bewertung erscheint bereits zweifelhaft, ob bei einem Zahlungskartenmissbrauch aufgrund einer Skimming-Attacke die Voraussetzungen für die Annahme eines Anscheinsbeweises bejaht werden könnten, wenn der Karteninhaber weiterhin im Besitz der Karte ist. Jedenfalls läge es in solchen Fällen aber nahe, dass für den Missbrauch andere Ursachen als eine grob fahrlässige Sorgfaltspflichtverletzung des Kunden in Betracht kommen. Wie bereits in der Antwort zu Frage 2 dargestellt, können Transaktionen mit (auch vom Chip) ab-

gegriffenen Magnetstreifendaten nur aus Ländern außerhalb der SEPA-Zone erfolgreich sein. Diese werden im Regelfall kaum mit in Deutschland befindlichen Bankkunden in Verbindung gebracht werden können, die weiterhin im Besitz der Originalkarte sind. Das Institut des Anscheinsbeweises ermöglicht es dem erkennenden Richter daher, flexibel auf neuere Entwicklungen zu reagieren und den Besonderheiten des jeweiligen Einzelfalles gerecht werdende Ergebnisse zu erzielen. Ein gesetzgeberischer Handlungsbedarf wird daher insoweit nicht gesehen.

11. Wurden und werden Mittel aus dem Bundeshaushalt (z. B. im Bereich der Sicherheitsforschung) zur Entwicklung sicherer Bankautomatentransaktionen verwendet, und wenn ja, in welcher Höhe?

Nein.

12. Wie erklärt sich die Bundesregierung die ausbleibende Reaktion auf die 2006 bekannt gewordenen Sicherheitsprobleme, und hat die Bundesregierung in dieser Sache irgendetwas unternommen?

    Wenn ja, was?

Der Bundesregierung liegen keine Kenntnisse darüber vor, ob und inwieweit die Hersteller von Geldautomaten oder Kreditinstitute auf den dargelegten Sachverhalt reagiert haben. Die Bunderegierung selbst hat den Zentralen Kreditausschuss und Vertreter von Geldautomatenherstellern zu einem Runden Tisch eingeladen und insbesondere gegenüber den Vertretern der Kreditwirtschaft die Forderungen des Bundeskriminalamts bekräftigt, auf den Magnetstreifen auf Karten zu verzichten.

13. In welchen Ländern des einheitlichen Euro-Zahlungsraumes, und in welchen anderen Ländern sind derzeit Karten ohne Magnetstreifen überhaupt, und in welchem Ausmaß einsetzbar?

Der Bunderegierung liegen hierzu keine Detailinformationen vor.

14. Erforschen BKA und das Bundesamt für Sicherheit in der Informationstechnik die Sicherheitsprobleme mit Bankkarten, und wenn ja, in welcher Form, seit wann, in welchem Umfang, und mit welchem Aufwand?

Das BKA erforscht ständig mögliche Sicherheitslücken von Zahlungskarten, um frühzeitig Gegenstrategien entwickeln zu können. Dies gilt insbesondere im Hinblick auf die Umstellung der Zahlungskarten auf Chipkartentechnologie. Das Bundesamts für Sicherheit in der Informationstechnik analysiert im Auftrag von Gerichten die Sicherheit von PIN-Verfahren.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333